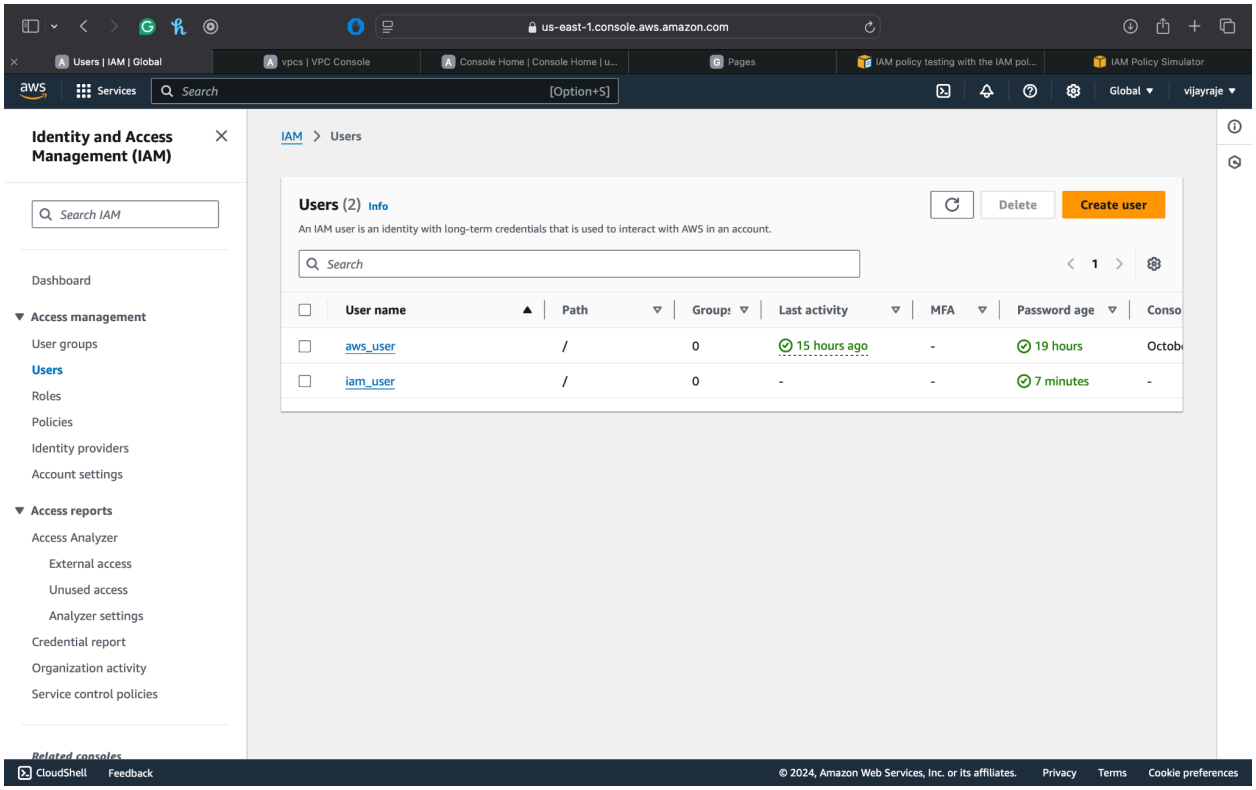
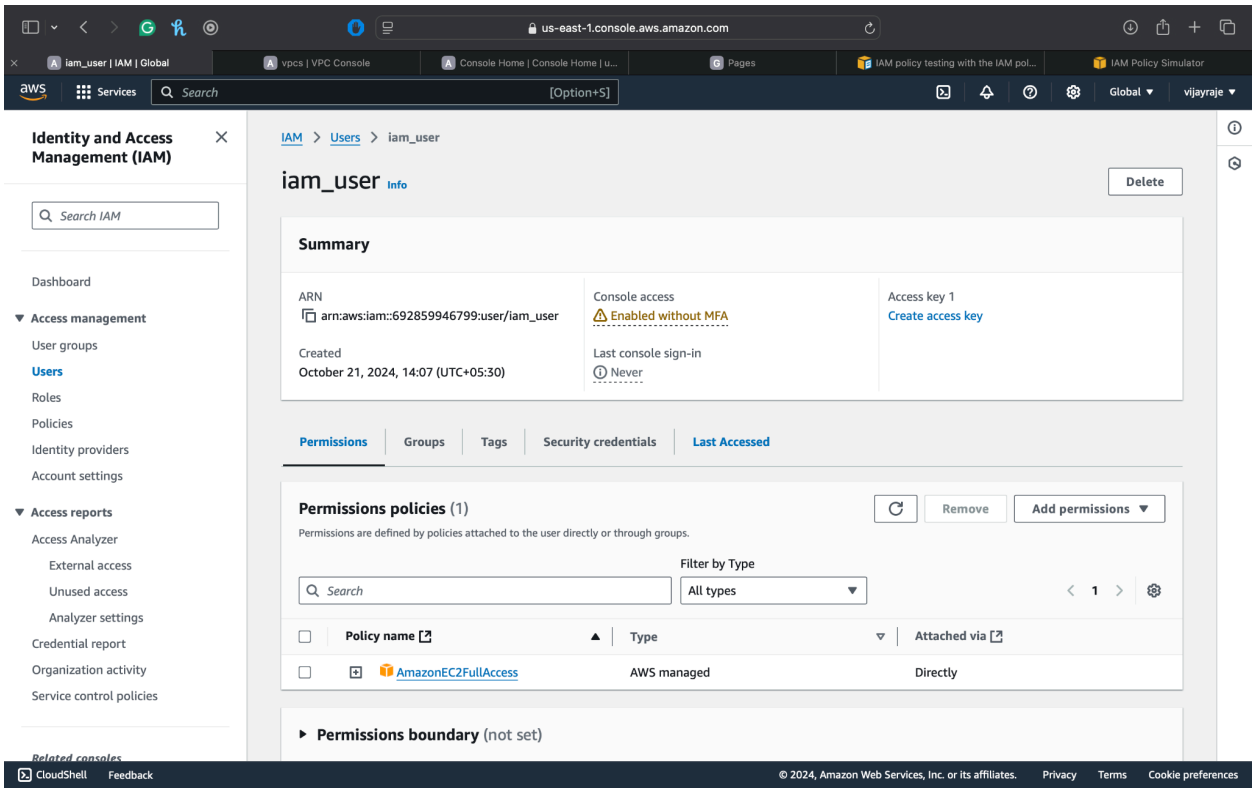
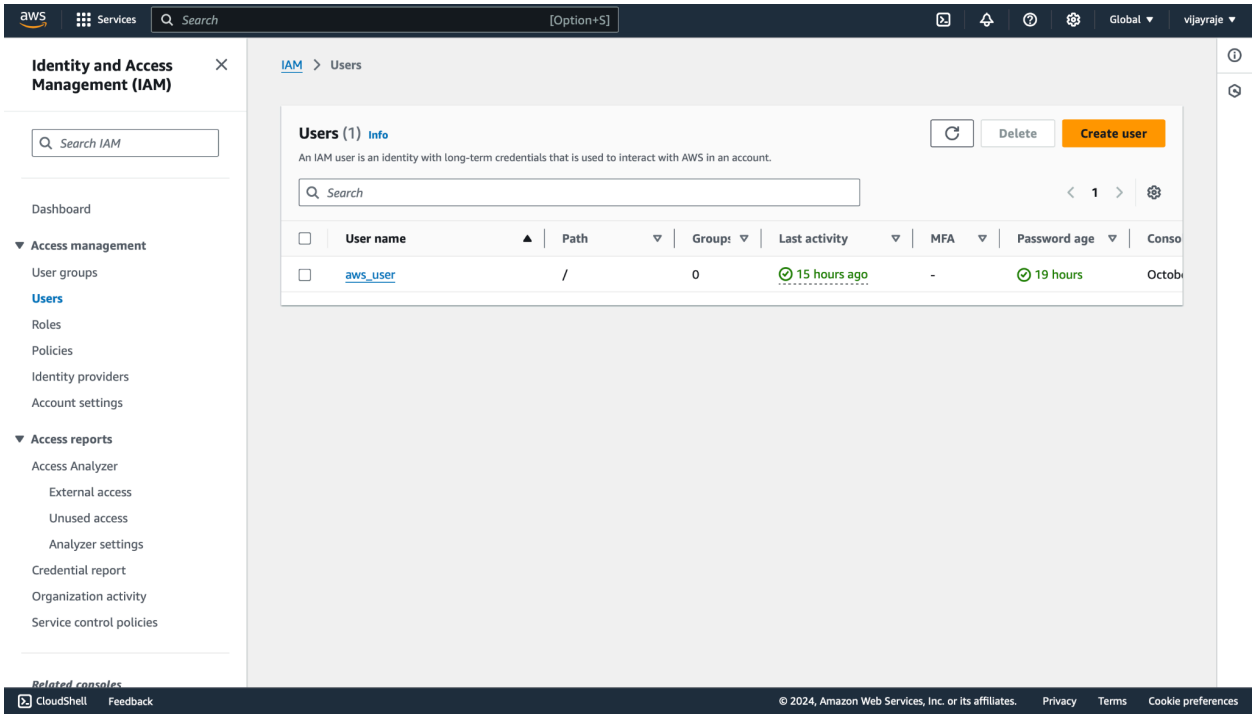
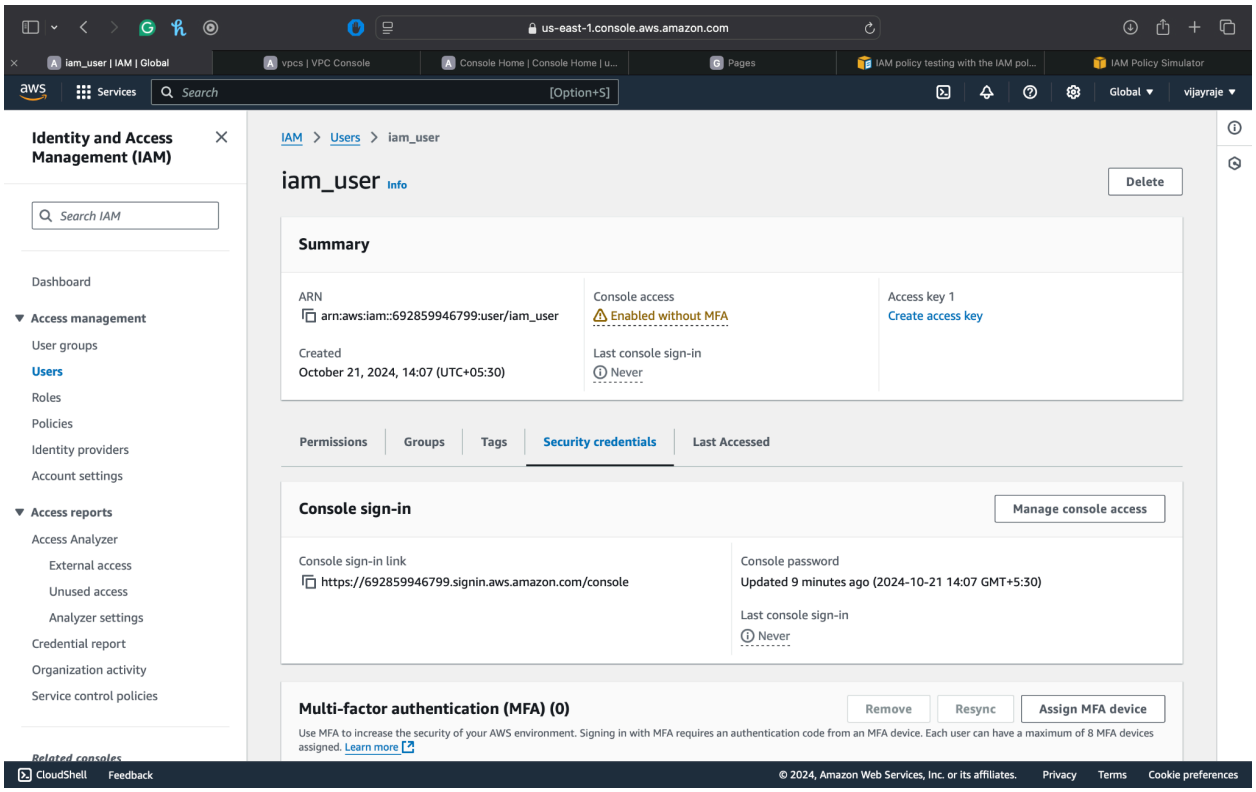
AWS


us-east-1.console.aws.amazon.com
Users | IAM | Global
vpcs | VPC Console
Console Home | Console Home | u...
Pages
IAM policy testing with the IAM pol...
IAM Policy Simulator
Services
Search
[Option+S]
Global
vijayraje
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
IAM > Users
Users (2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
1
User name
Path
Groups
Last activity
MFA
Password age
aws_user
/
0
15 hours ago
-
19 hours
iam_user
/
0
-
-
7 minutes
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

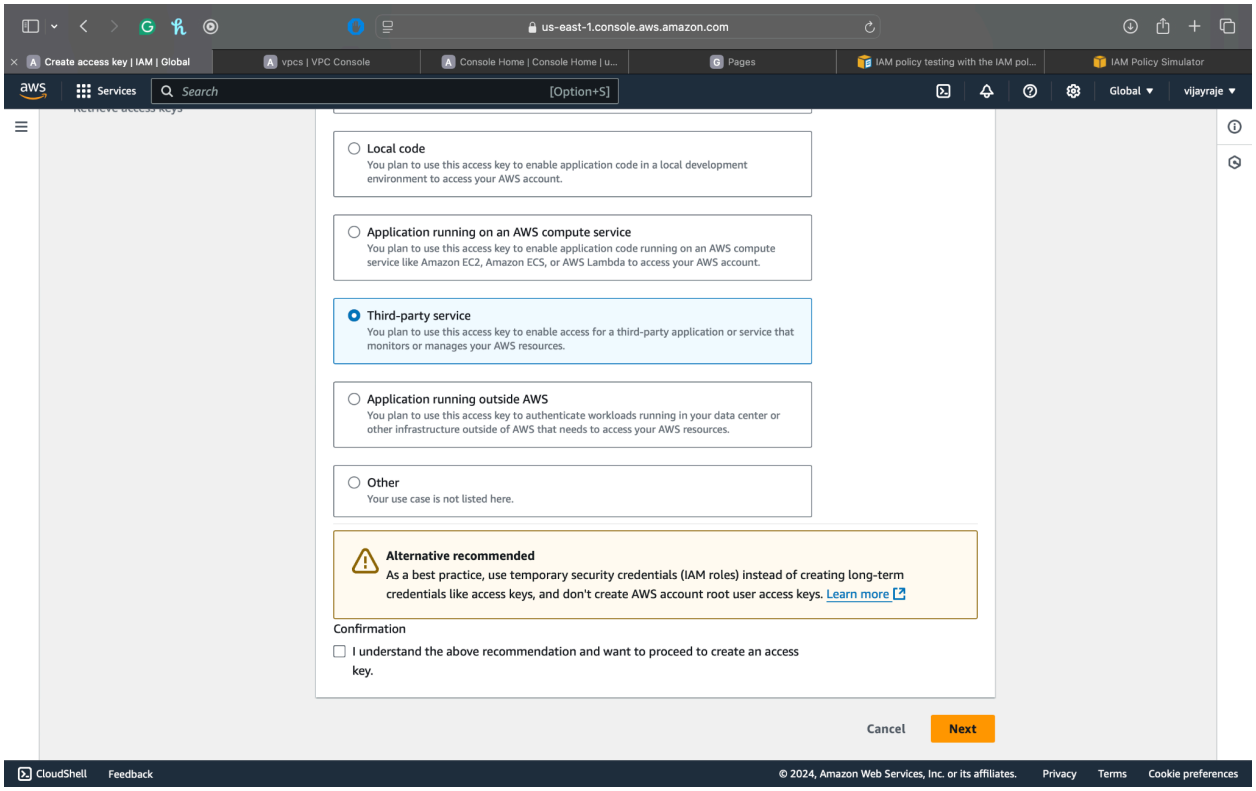

us-east-1.console.aws.amazon.com
iam_user | IAM | Global
vpcs | VPC Console
Console Home | Console Home | u...
Pages
IAM policy testing with the IAM pol...
IAM Policy Simulator
Services
Search
[Option+S]
Global
vijayraje
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
IAM > Users > iam_user
iam_user Info
Delete
Summary
ARN
arn:aws:iam::692859946799:user/iam_user
Console access
Enabled without MFA
Access key 1
Create access key
Created
October 21, 2024, 14:07 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
1
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
Permissions boundary (not set)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

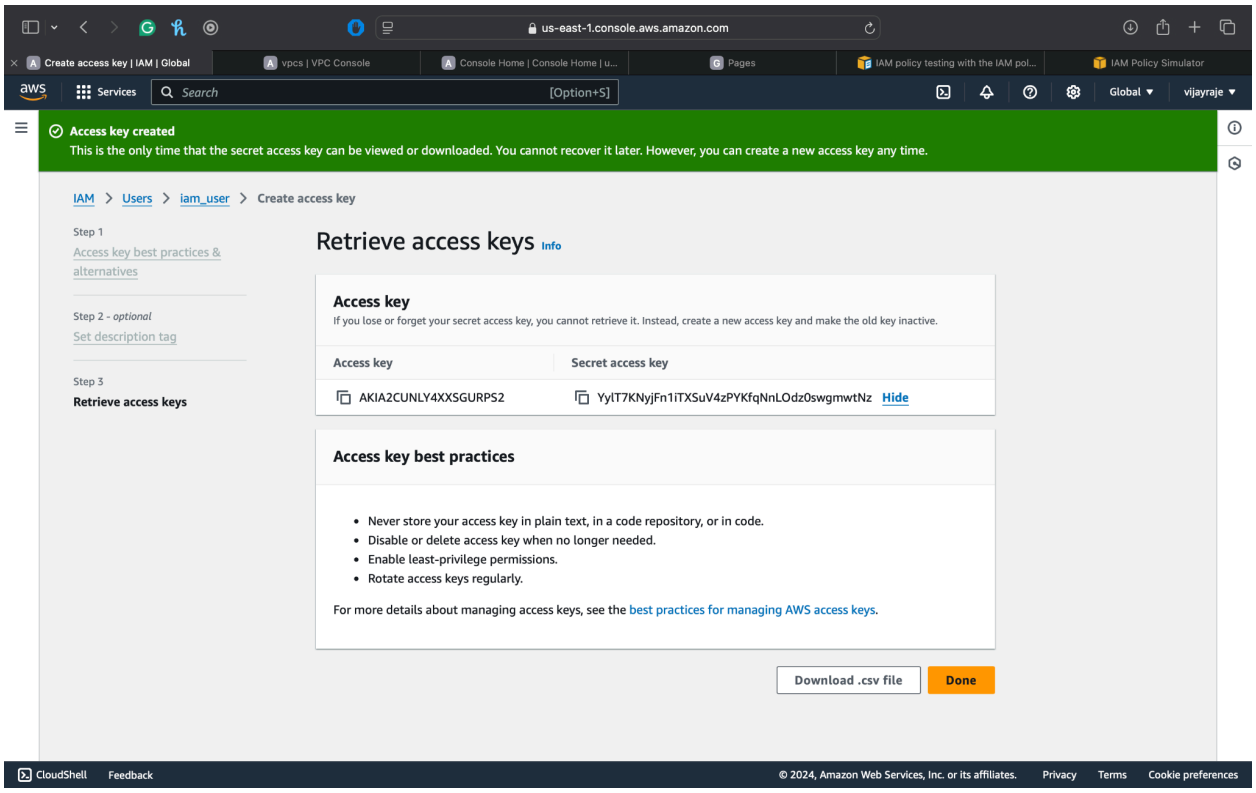


Console access granted

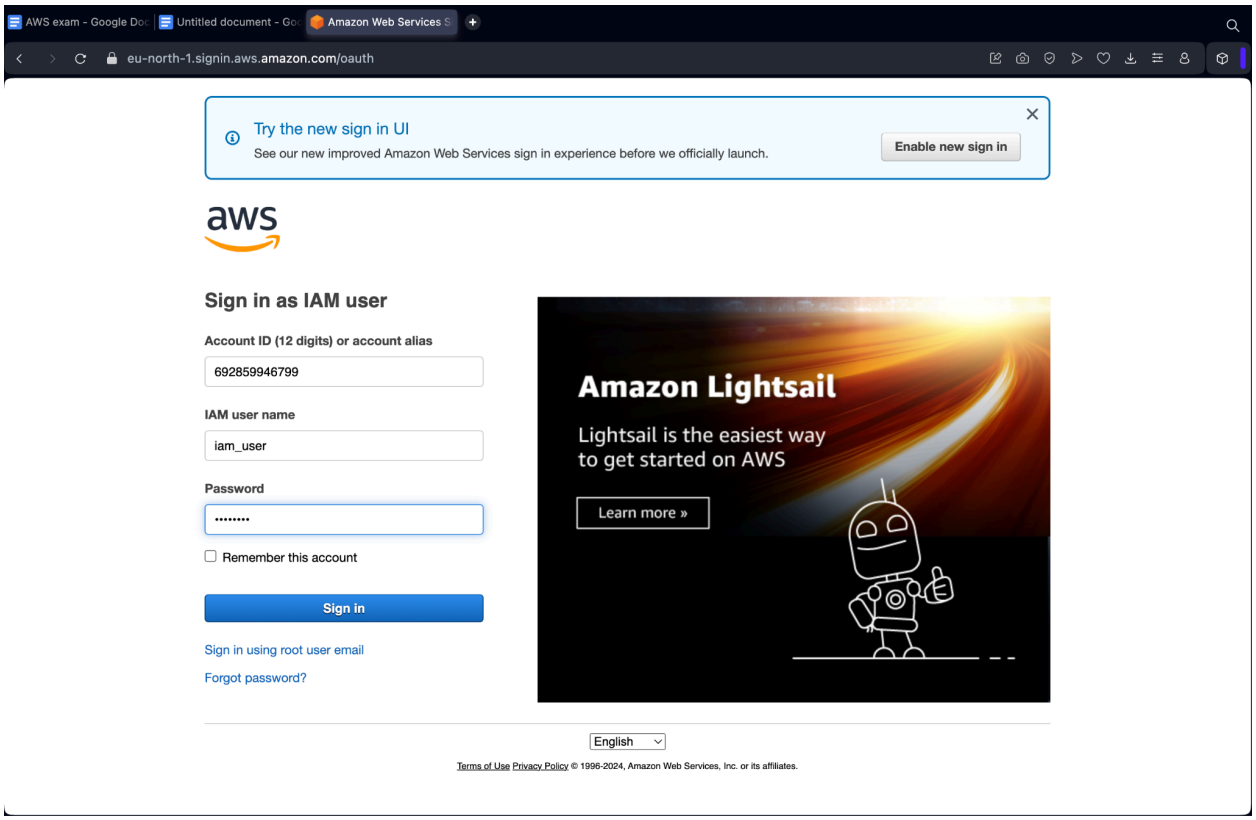


Acces key generation

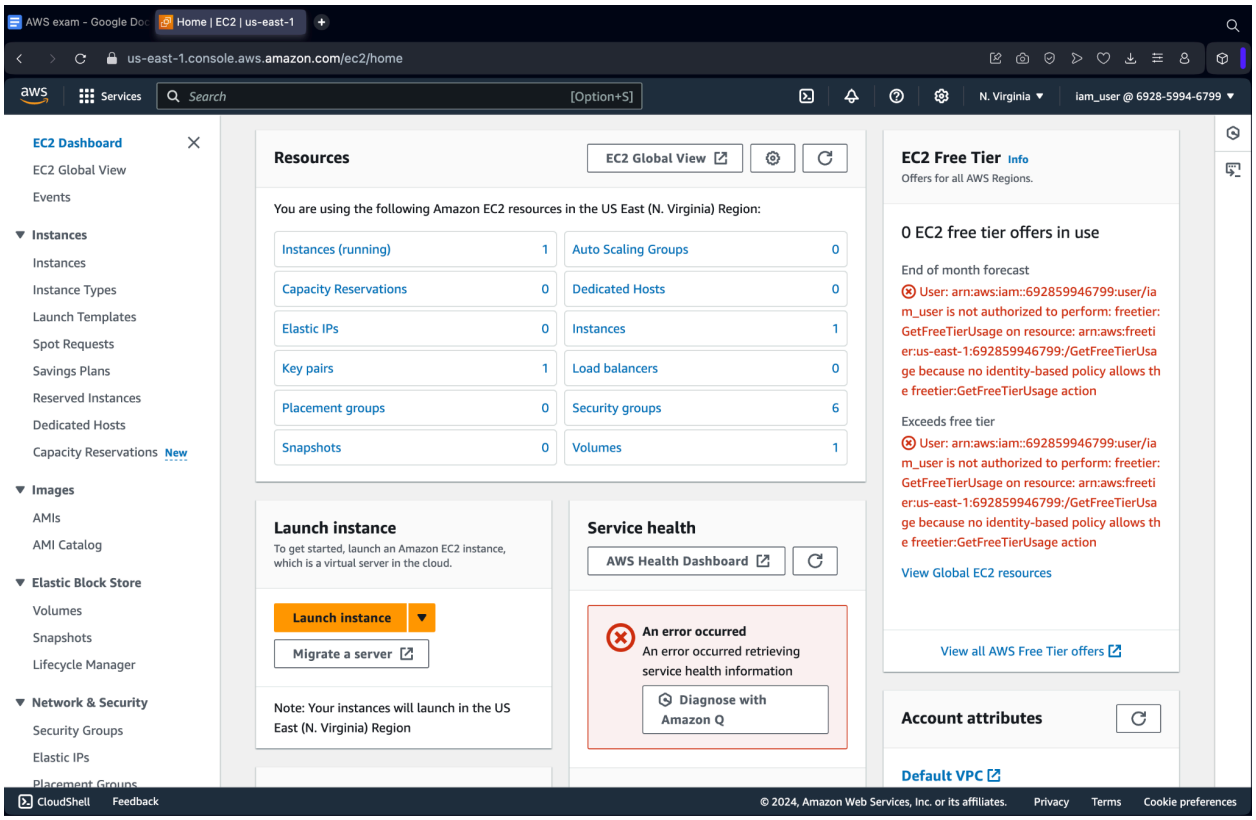




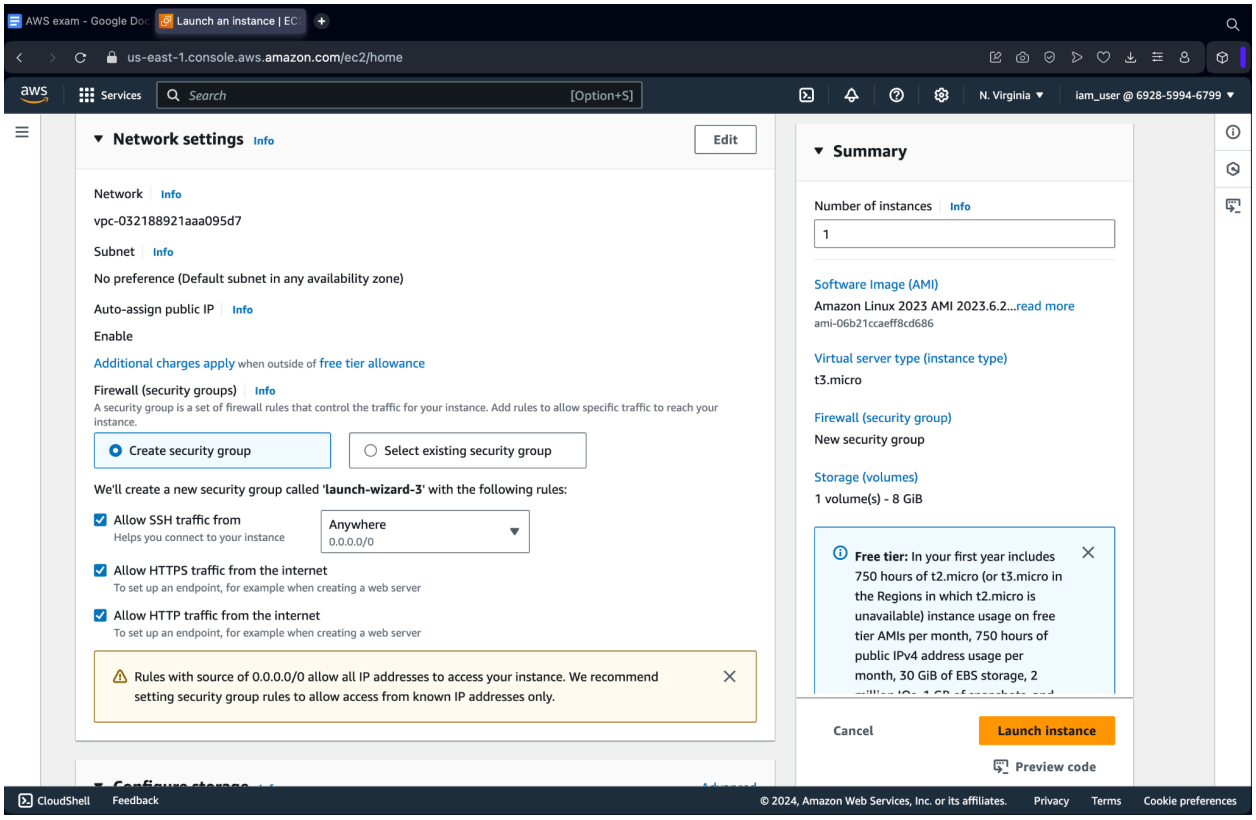
I am user login

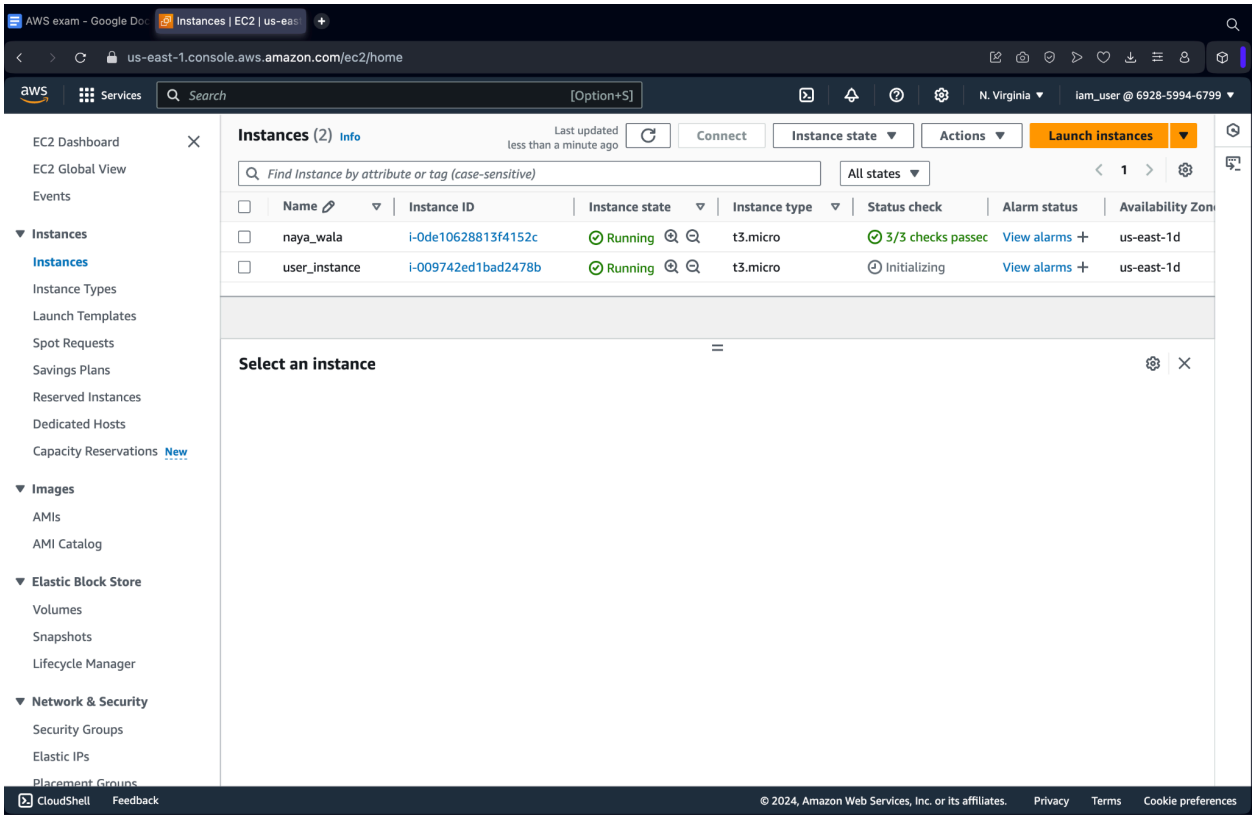


Can access the ec2 instance my the user

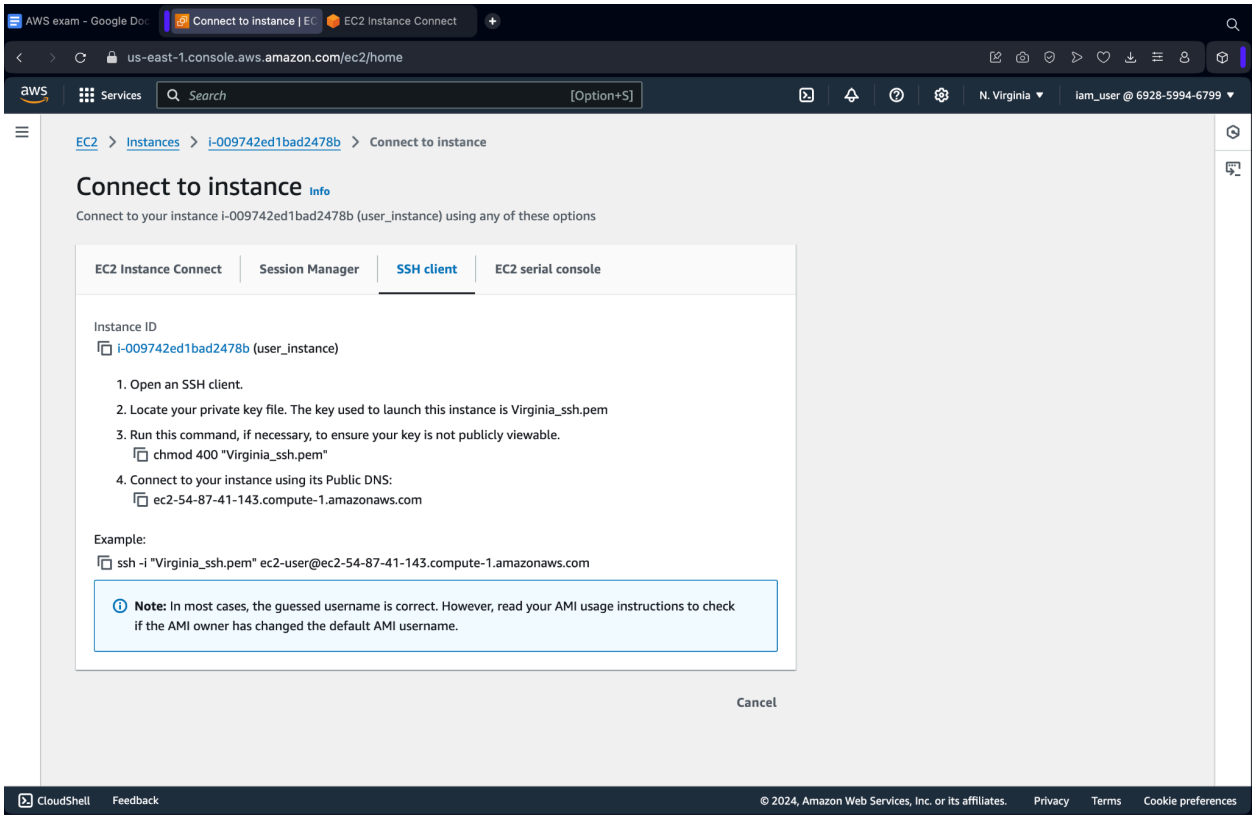


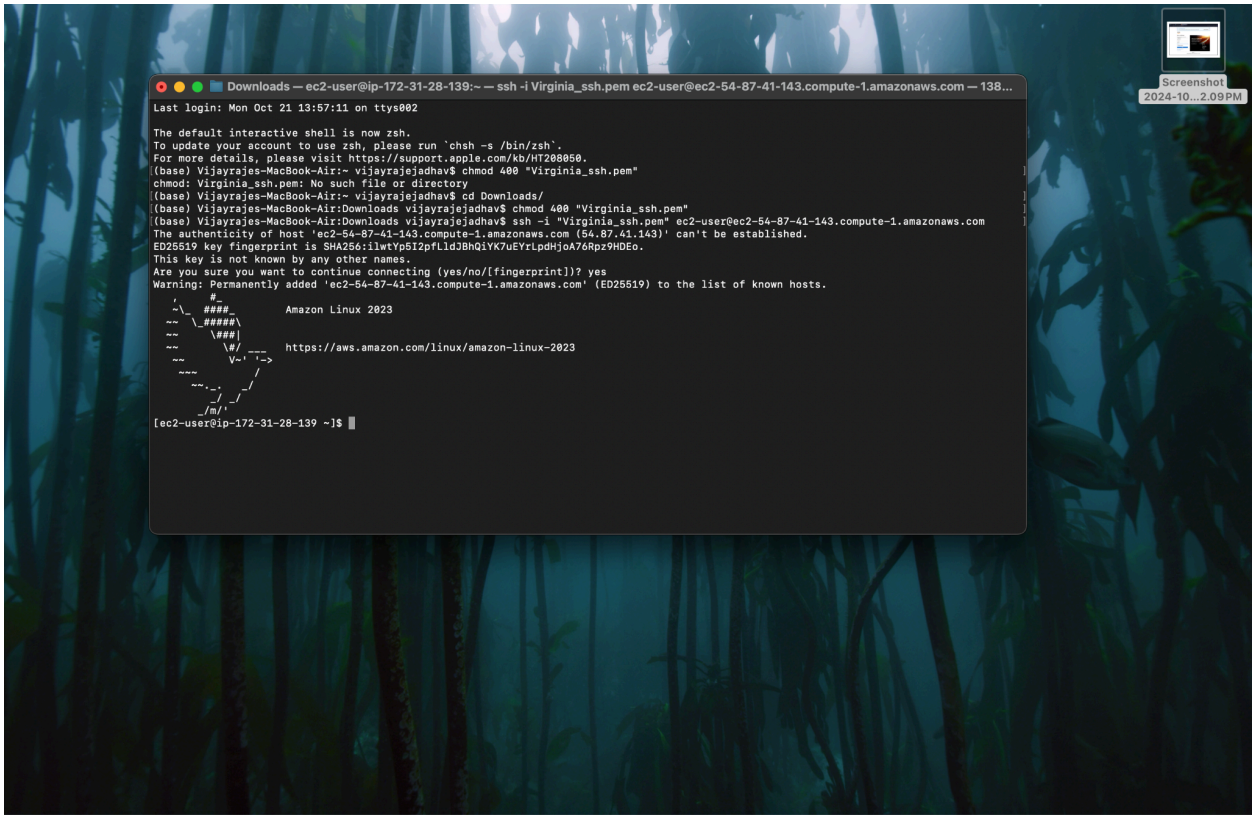
He can create the instance



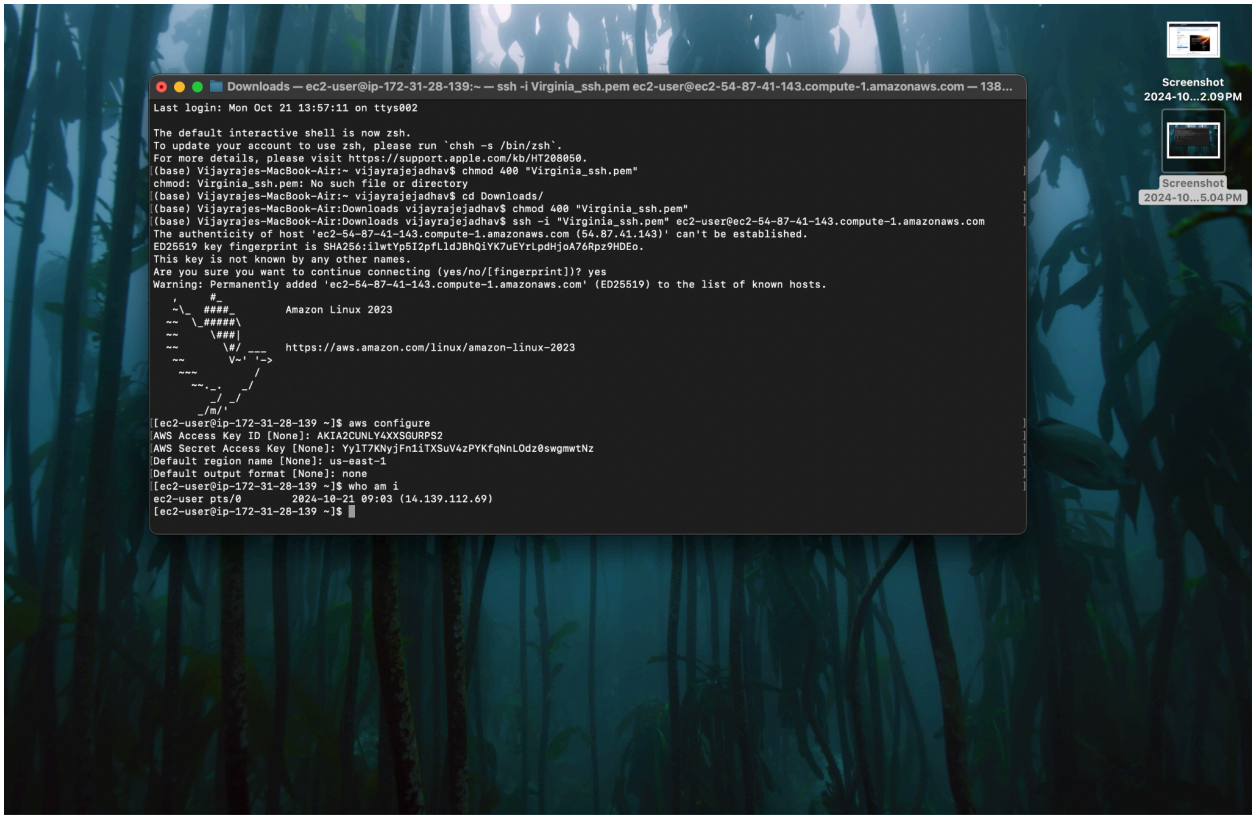


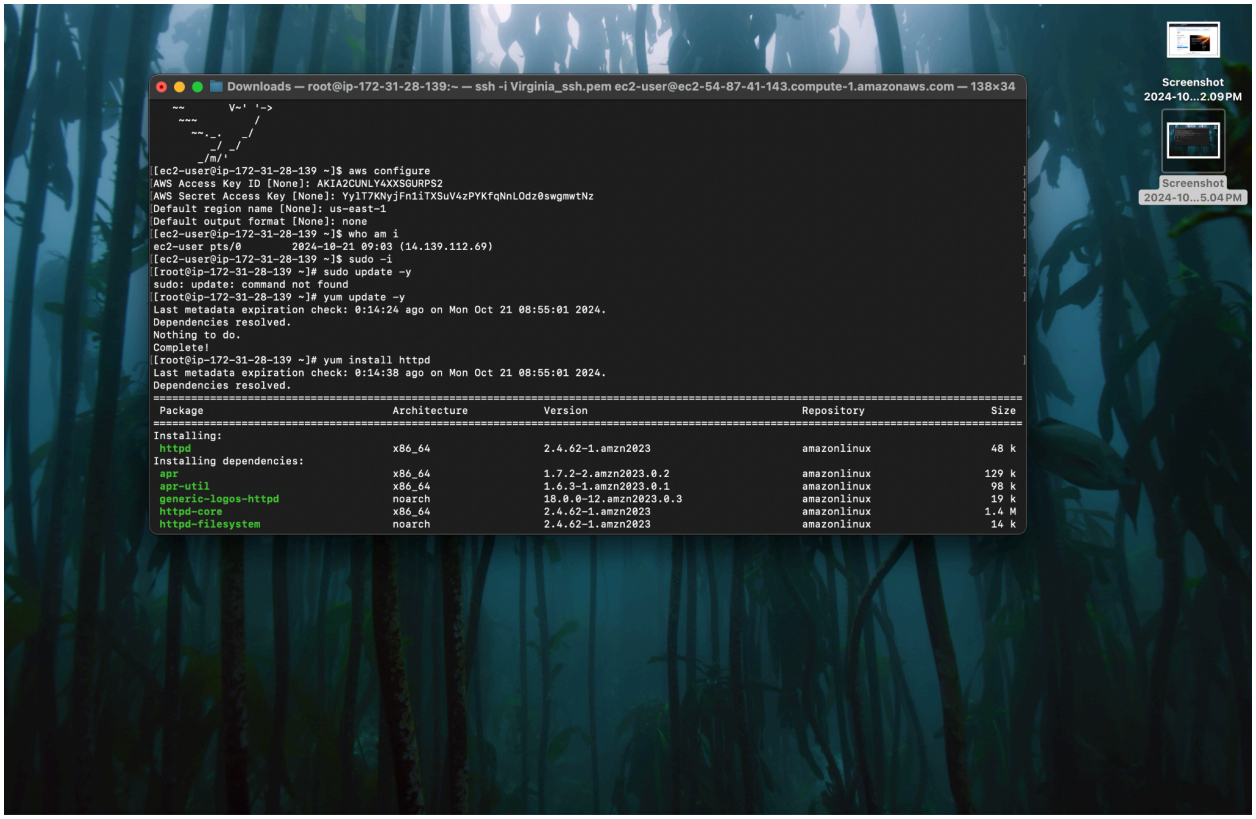
Connect with ssh



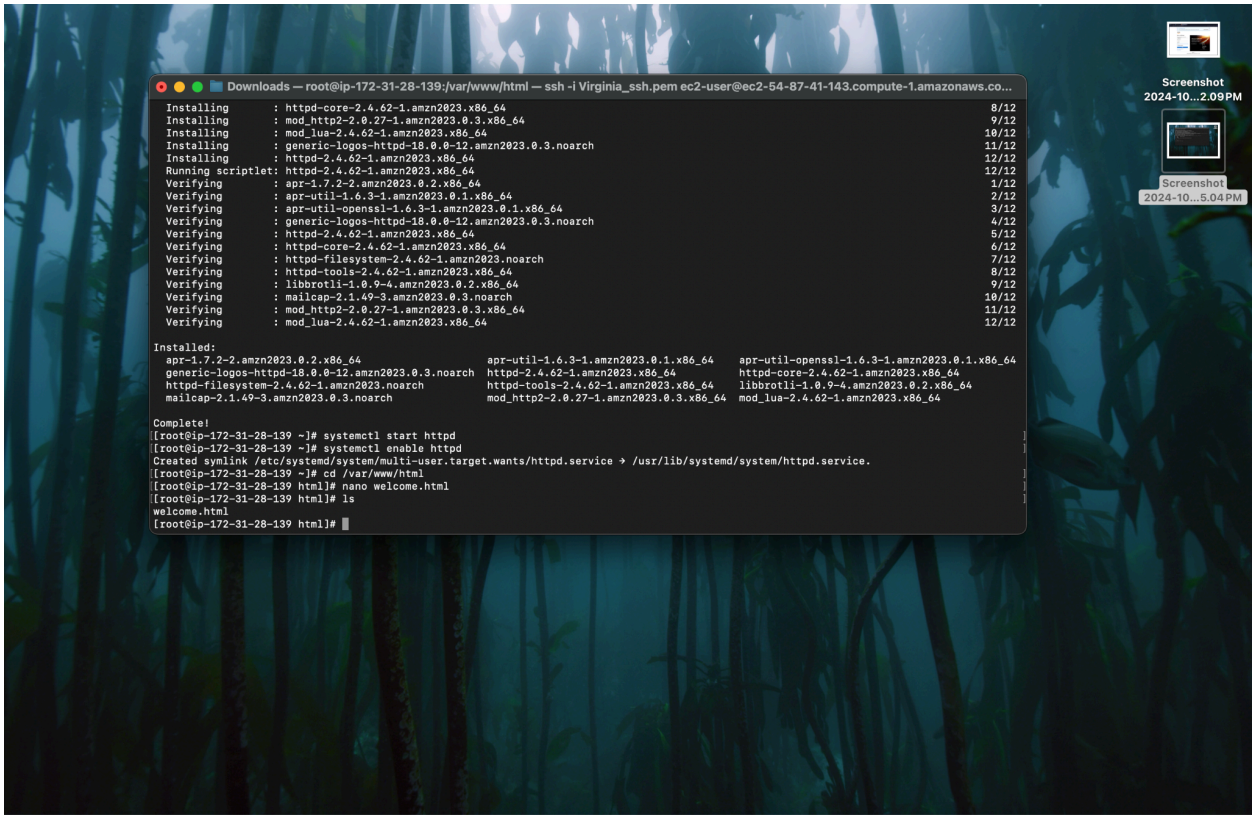


The iam user successfully accessed the ec2 instance with access key

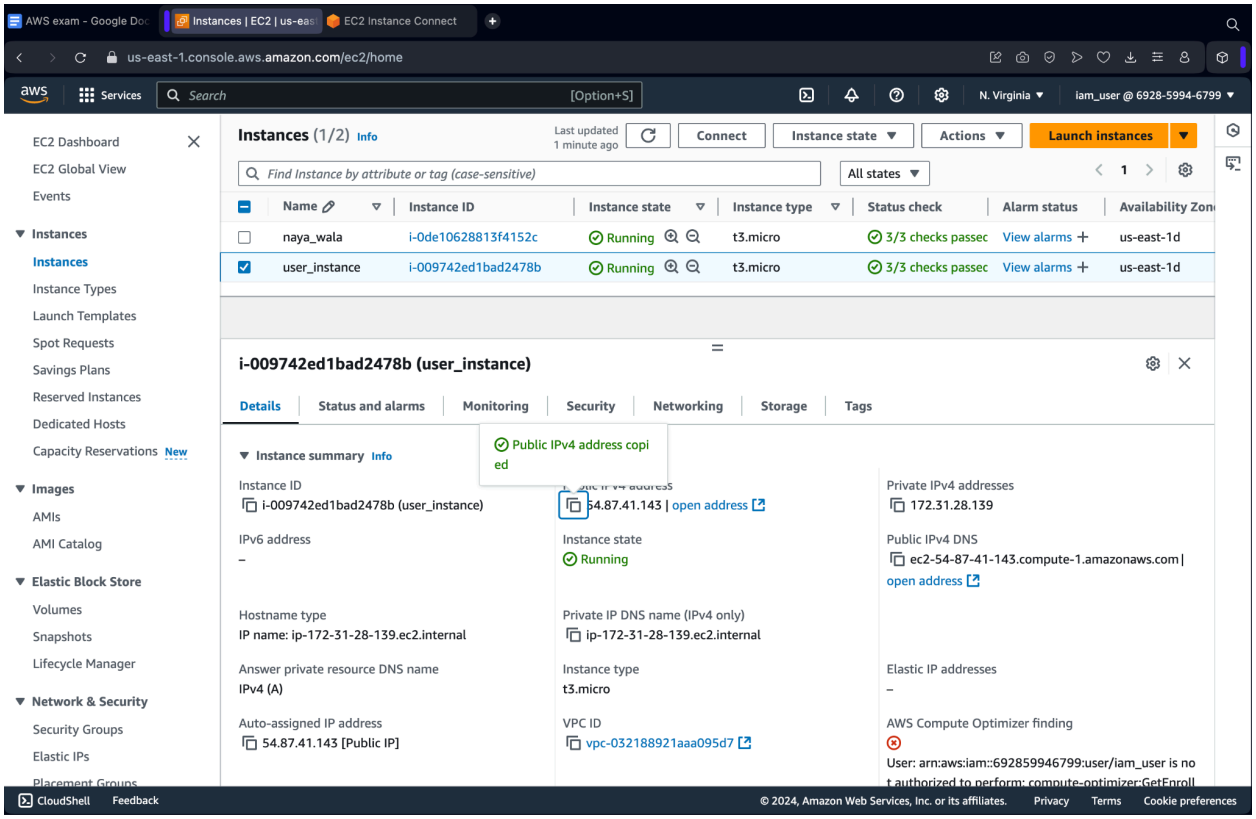


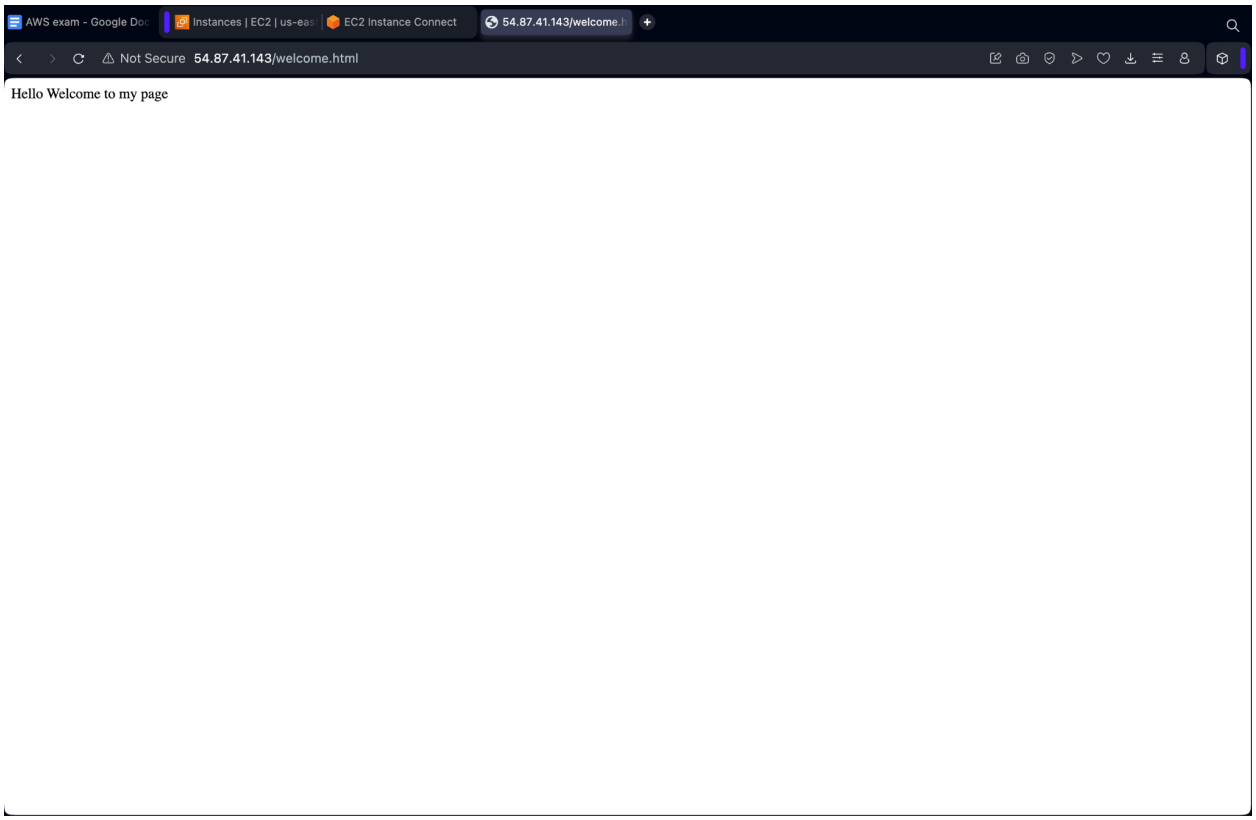


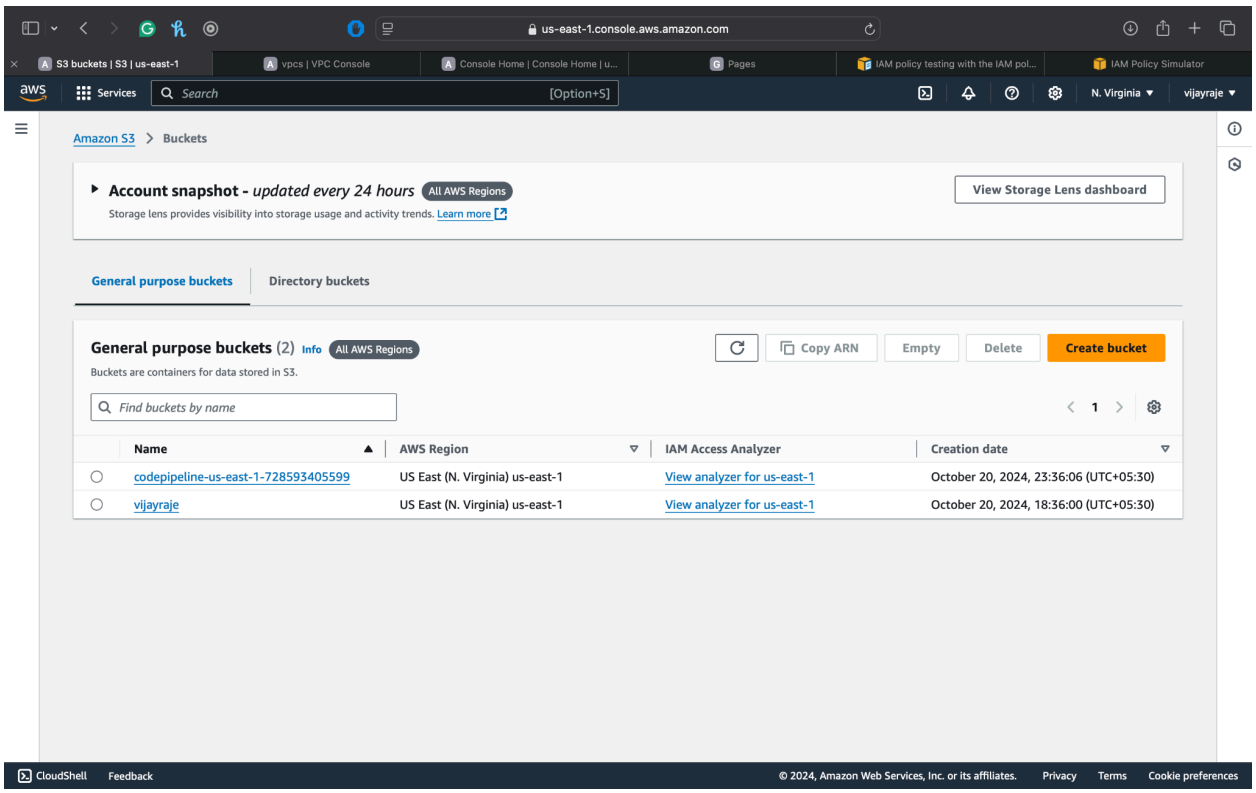
Start and install httpd

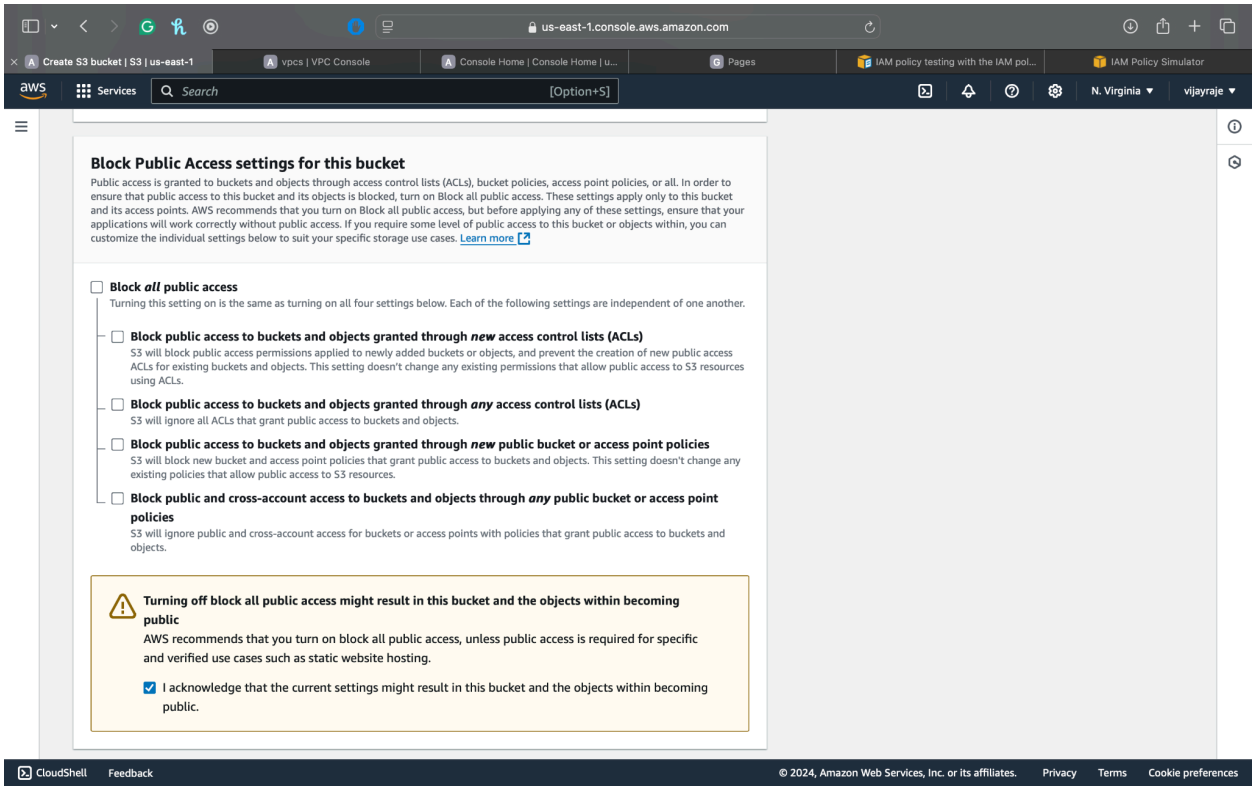


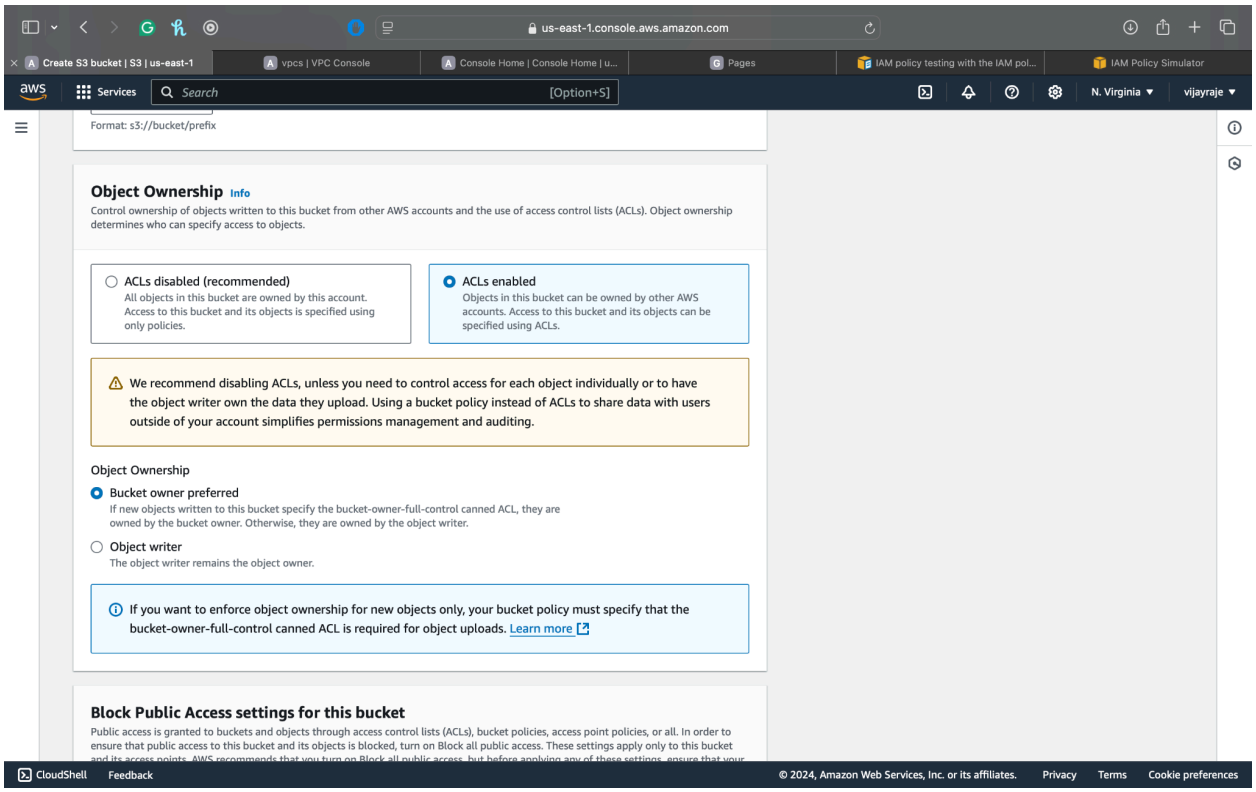
The webpage can be accessed by instance ip

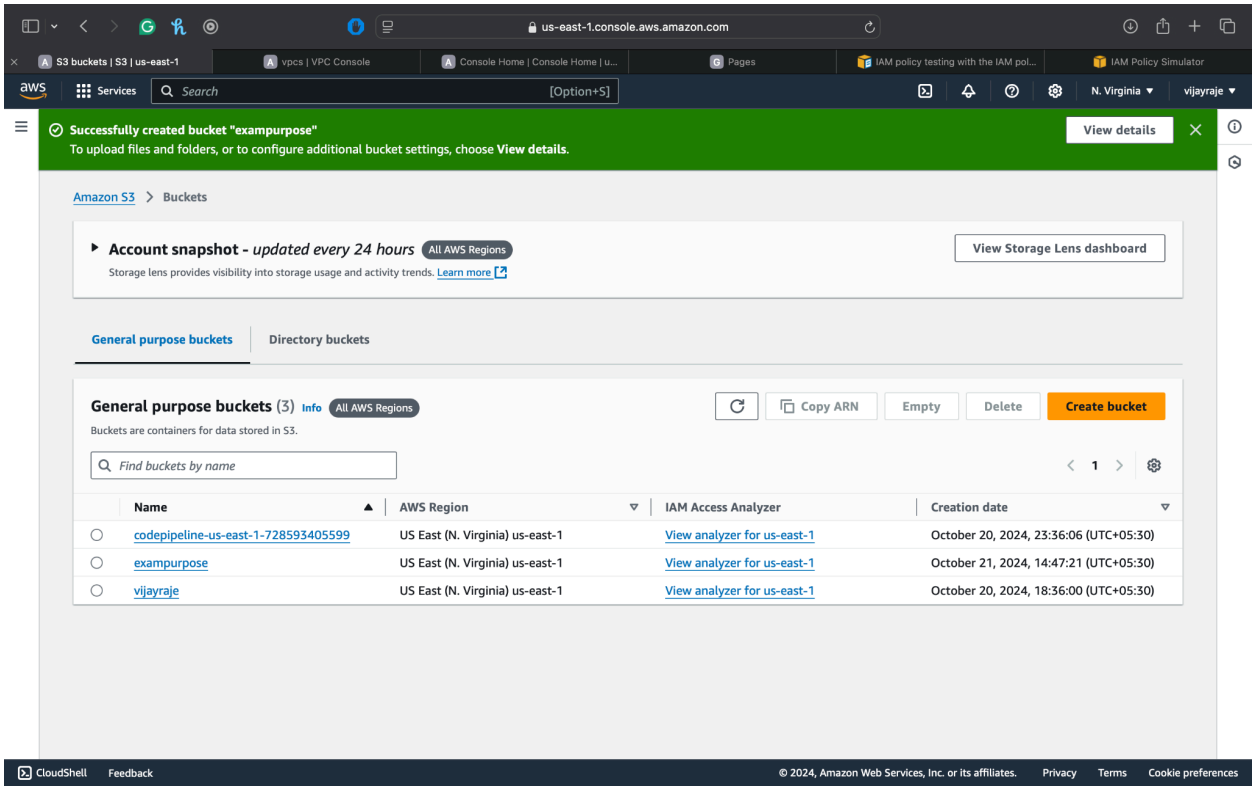


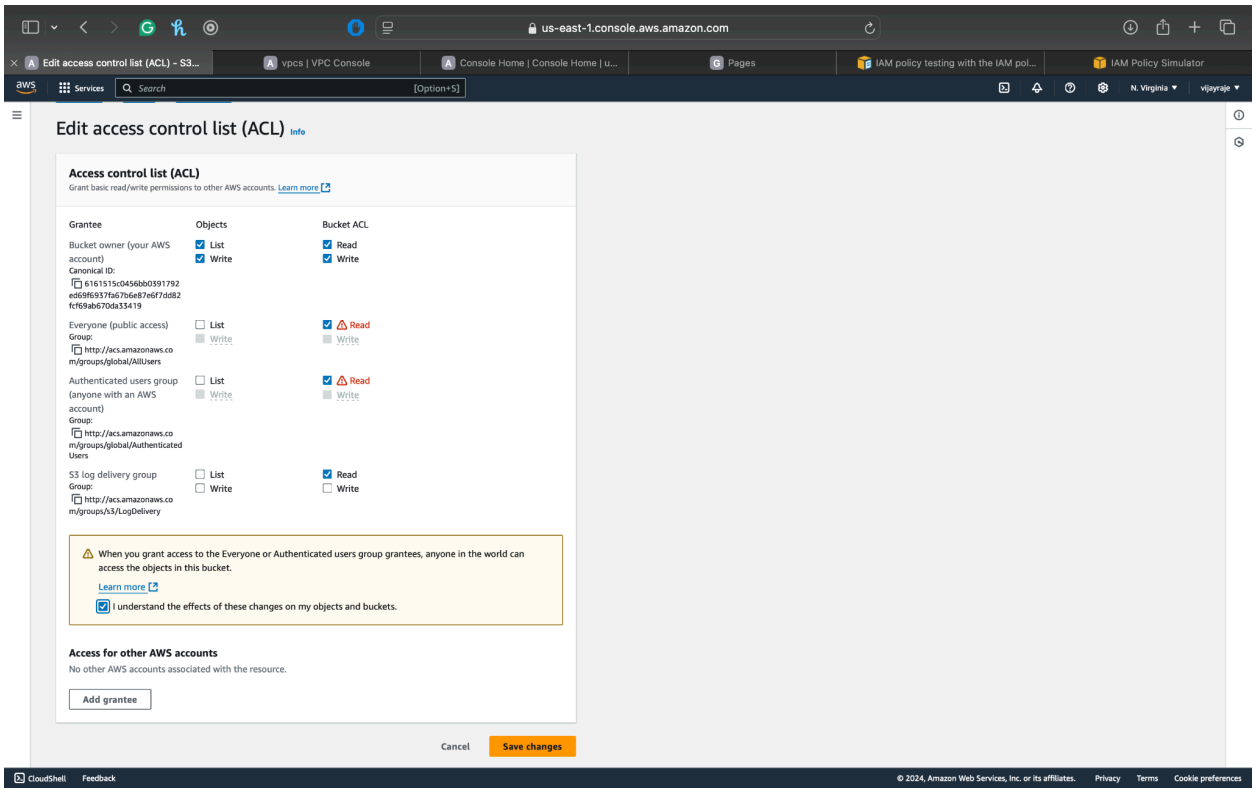

AWS exam - Google Doc
Instances | EC2 | us-eas
EC2 Instance Connect
54.87.41.143/welcome.h
Not Secure 54.87.41.143/welcome.html
Hello Welcome to my page


us-east-1.console.aws.amazon.com
S3 buckets | S3 | us-east-1
vpcs | VPC Console
Console Home | Console Home | u...
Pages
IAM policy testing with the IAM pol...
IAM Policy Simulator
aws
Services
Search
[Option+S]
N. Virginia
vijayraje
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (2) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
IAM Access Analyzer
Creation date
codepipeline-us-east-1-728593405599
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 20, 2024, 23:36:06 (UTC+05:30)
vijayraje
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 20, 2024, 18:36:00 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

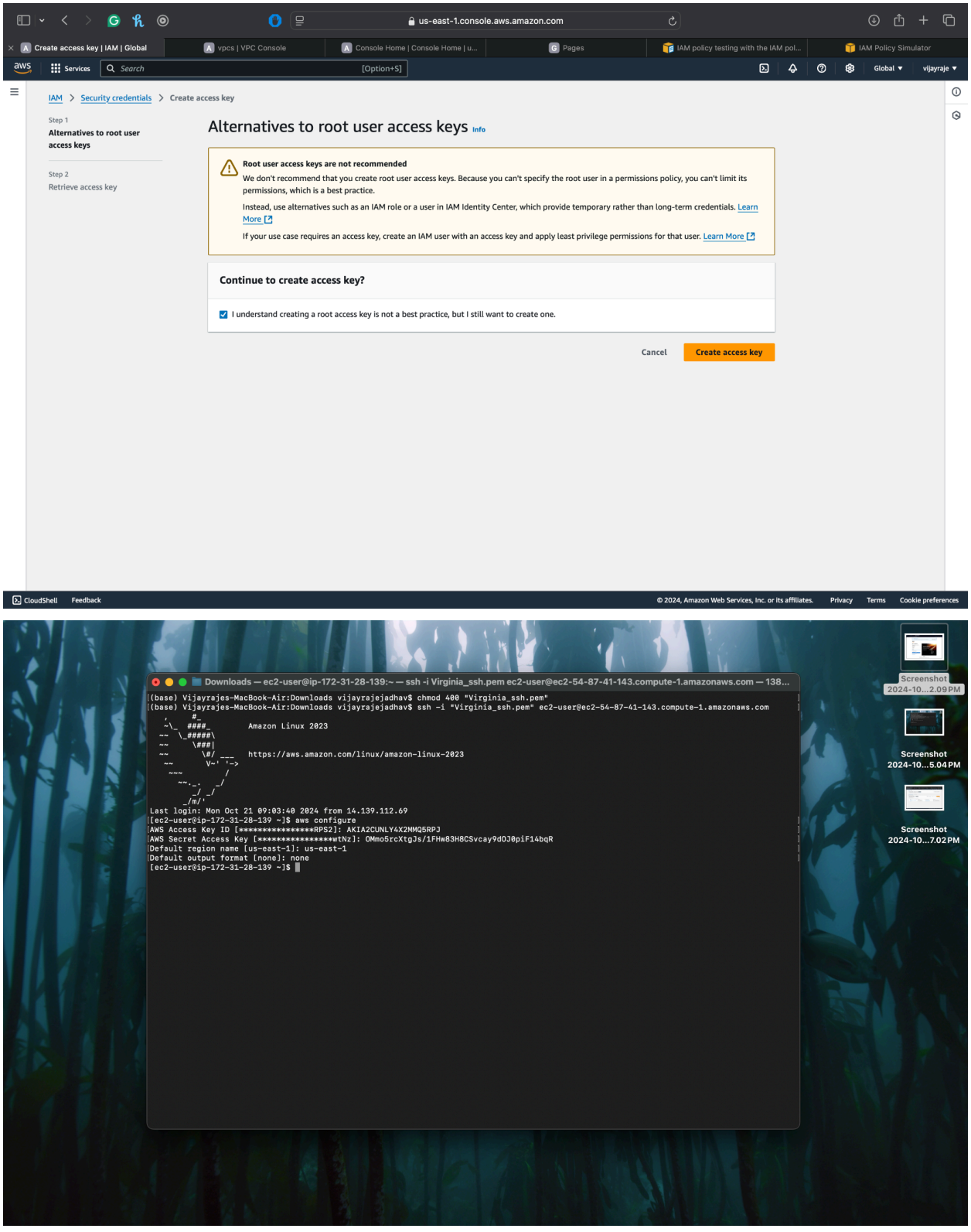

us-east-1.console.aws.amazon.com
Create S3 bucket | S3 | us-east-1
vpcs | VPC Console
Console Home | Console Home | u...
Pages
IAM policy testing with the IAM pol...
IAM Policy Simulator
Services
Search
[Option+S]
N. Virginia
vijayraje
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com
Create S3 bucket | S3 | us-east-1
vpcs | VPC Console
Console Home | Console Home | u...
Pages
IAM policy testing with the IAM pol...
IAM Policy Simulator
Services
Search
[Option+S]
N. Virginia
vijayraje
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
The object writer remains the object owner.
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com
S3 buckets | S3 | us-east-1
vpcs | VPC Console
Console Home | Console Home | u...
Pages
IAM policy testing with the IAM pol...
IAM Policy Simulator
Services
Search
[Option+S]
N. Virginia
vijayraje
Successfully created bucket "exampurpose"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (3) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
codepipeline-us-east-1-728593405599
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 20, 2024, 23:36:06 (UTC+05:30)
exampurpose
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 21, 2024, 14:47:21 (UTC+05:30)
vijayraje
US East (N. Virginia) us-east-1
View analyzer for us-east-1
October 20, 2024, 18:36:00 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

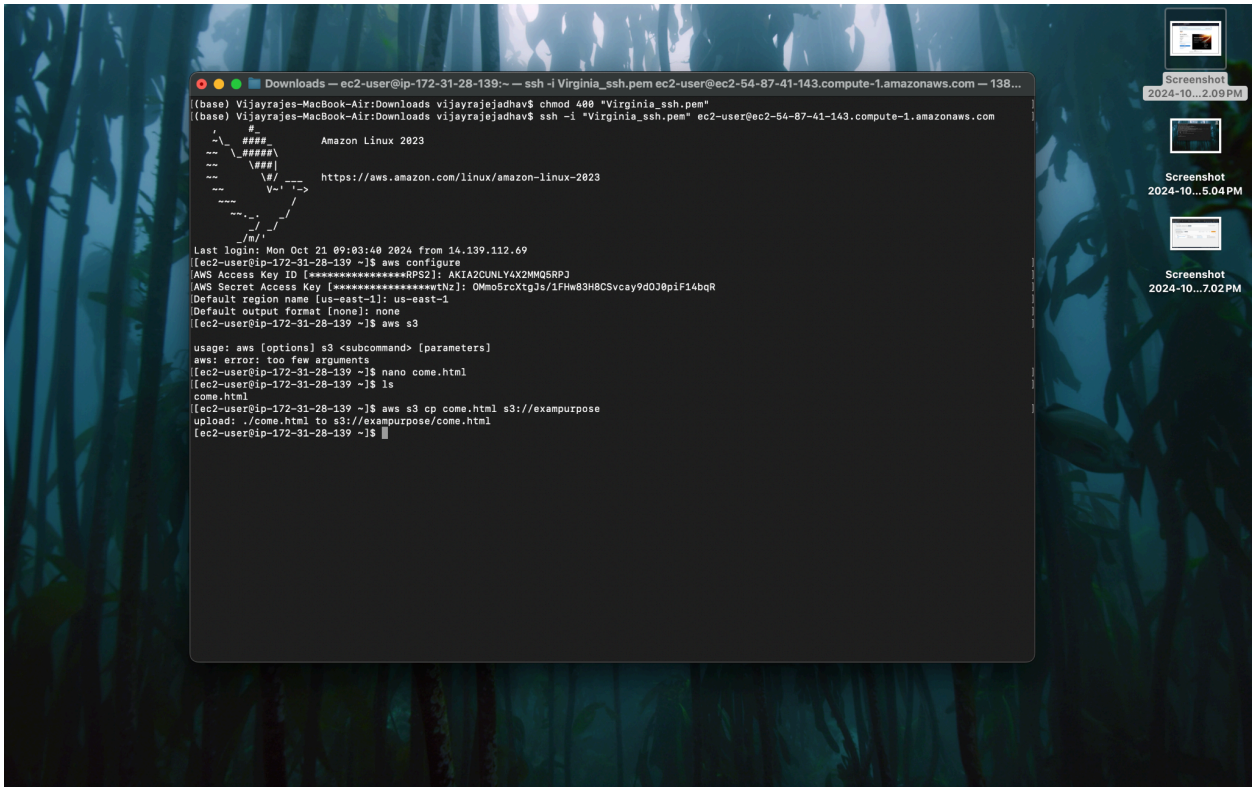

us-east-1.console.aws.amazon.com
Edit access control list (ACL) - S3...
Edit access control list (ACL) Info
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID:
6161515c0456bb0391792ed69f6937fa67b6e876f7dd82fcf69ab670da33419
List
Write
Read
Write
Everyone (public access)
Group:
http://acs.amazonaws.com/groups/global/AllUsers
List
Write
Read
Write
Authenticated users group (anyone with an AWS account)
Group:
http://acs.amazonaws.com/groups/global/AuthenticatedUsers
List
Write
Read
Write
S3 log delivery group
Group:
http://acs.amazonaws.com/groups/s3/LogDelivery
List
Write
Read
Write
When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.
Learn more
I understand the effects of these changes on my objects and buckets.
Access for other AWS accounts
No other AWS accounts associated with the resource.
Add grantee
Cancel
Save changes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create access key for root user

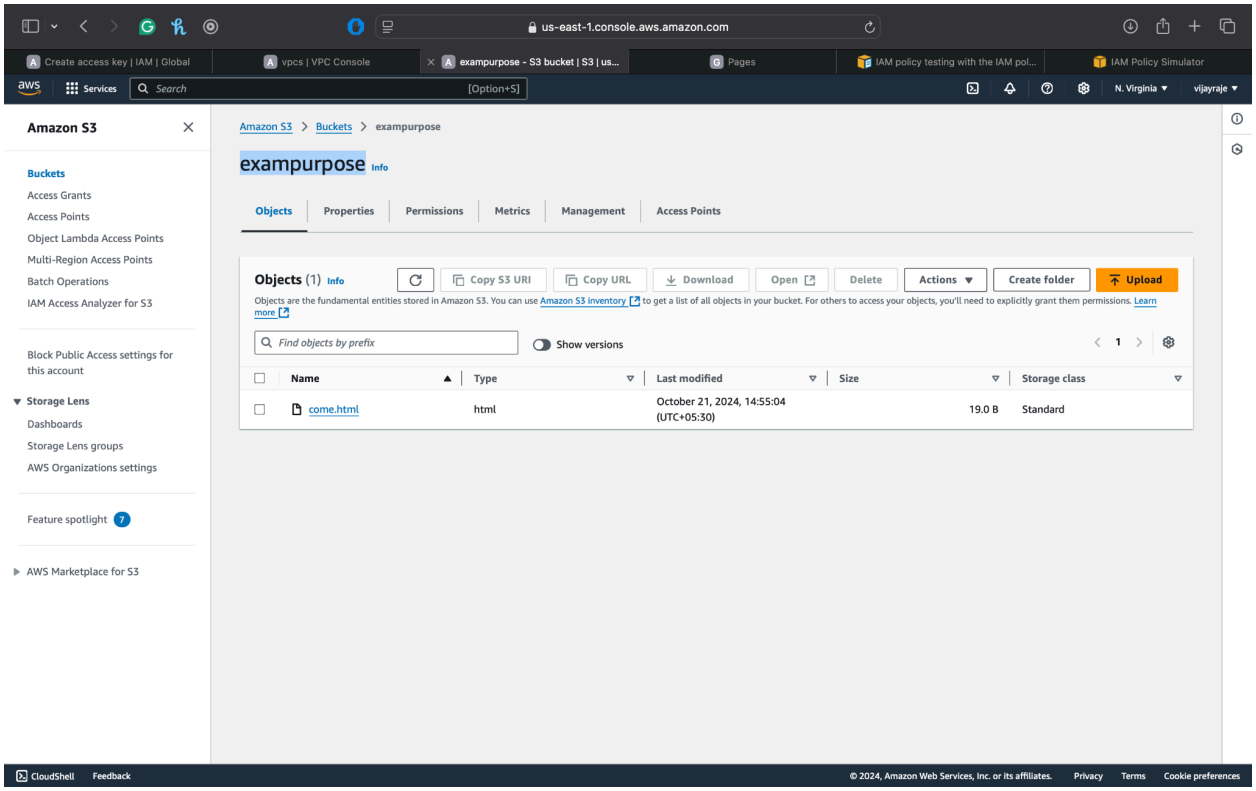


Get access through root id in instance

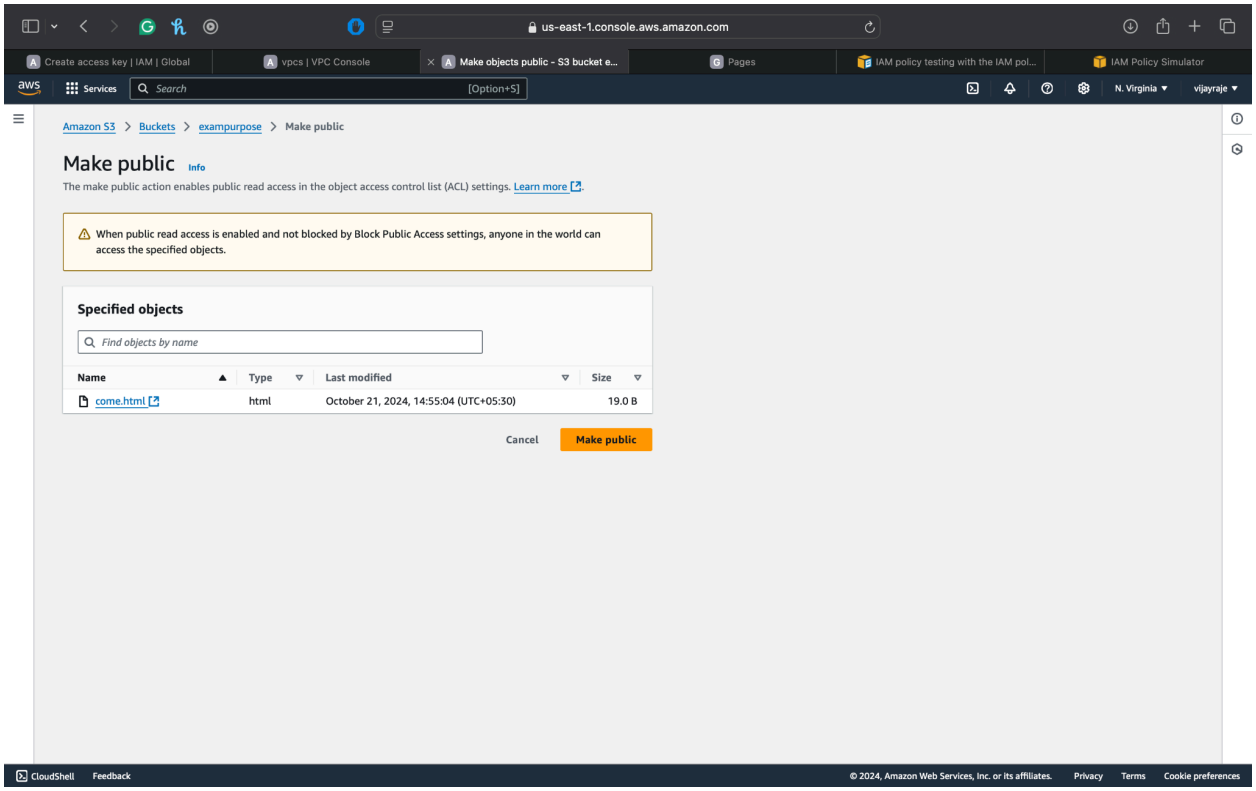
Upload the html file to the bucket



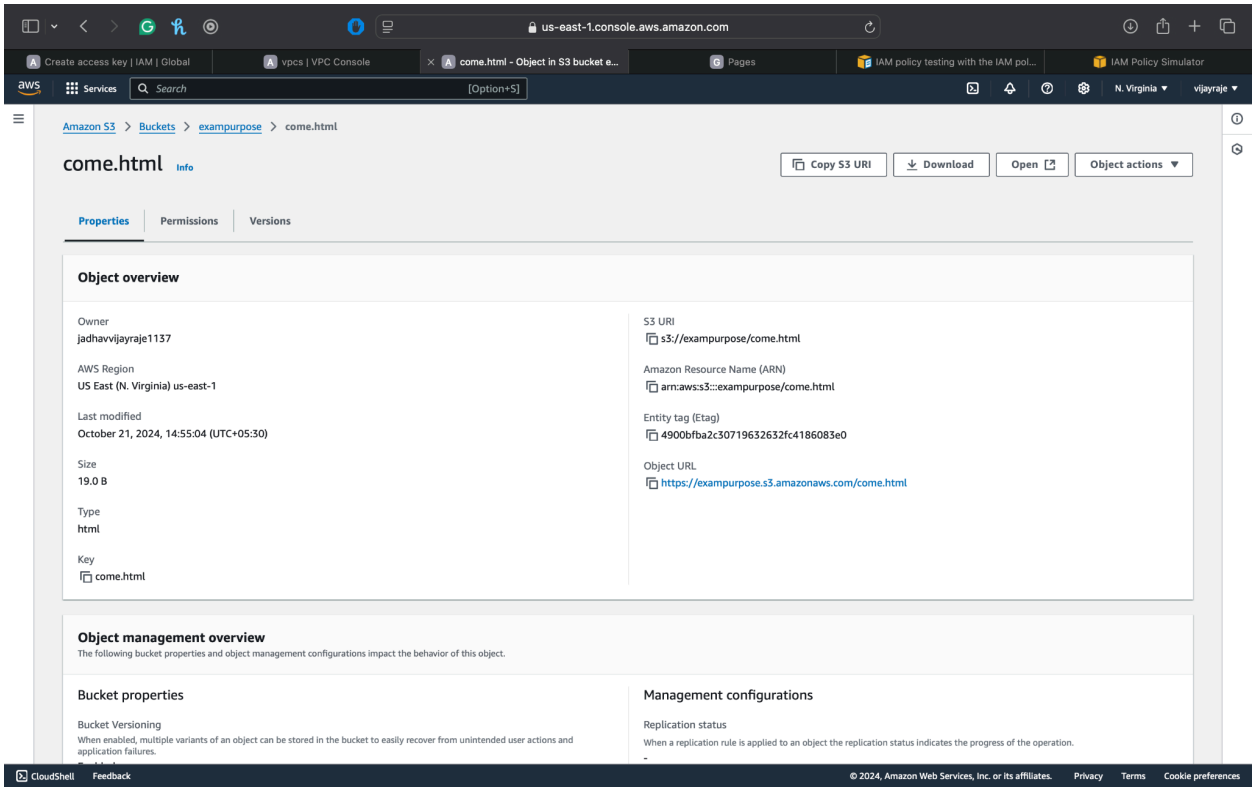
check the file in the bucket



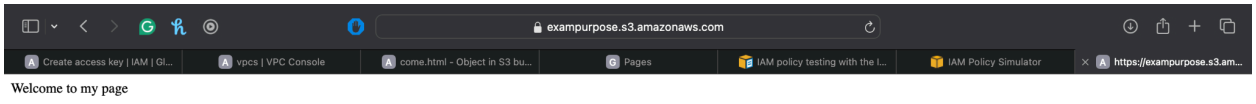
Make it public acl



Now copy the object url and check



It is working



https://exampurpose.s3.amazonaws.com/come.html

Url of that bucket